UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

CHARMENY LYONS, on behalf of herself, and on behalf of all others similarly situated, Plaintiff, v. ASCENSION HEALTH, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Charmeny Lyons ("Plaintiff"), by and through her attorneys of record, upon personal knowledge as to her own acts and experiences, and upon the investigation of counsel and information and belief as to all other matters, bring this class action complaint against defendant Ascension Health ("Ascension," or "Defendant"), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action on behalf of a Class, as defined below, against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' protected personal information stored within Defendant's information networks and servers, including, without limitation, "protected health information" ("PHI"),[1] and "personally identifiable

[1] Protected Health Information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient. PHI is inclusive of and incorporates personally identifiable information.

information" ("PII"),[2] as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, PHI and PII are also referred to therein as "Private Information").

2. Defendant is a large health care system and provider of health-care related services through its affiliated approximately 134,000 associates, 35,000 providers, and 140 hospitals. Defendant's health care system services patients in 19 states, including Wisconsin, and in the District of Columbia.[3]

3. In the course of providing services, Defendant acquired and collected Plaintiff's and Class Members' Private Information. Defendant knew, at all times material, that it was collecting, and responsible for the security of, sensitive data, including Plaintiff's and Class Members' highly confidential Private Information.

4. As Ascension acknowledged on its website 2024, Private Information in its possession was accessed and exfiltrated by unauthorized third persons – cyber-criminals – who target Private Information which is valuable to identity thieves. This unauthorized access was accomplished because Defendant failed to maintain appropriate and necessary safeguards, independent review, and oversight of the Private Information in its possession, and which still remains vulnerable to additional hackers and theft.

5. Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause them and thousands of other similarly situated persons by virtue of an unauthorized and preventable cyberattack that Defendant discovered by no later than May 8, 2024, when it detected "unusual activity on select technology network systems."

6. Plaintiff seeks to hold Defendant responsible for not ensuring that PII and PHI, as defined by HIPAA Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), and respecting which

---

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[3] https://about.ascension.org/news/media-resources, last visited May 23, 2024.

Defendant was duty bound to protect pursuant to the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), was maintained in a manner consistent with industry standards, and other relevant standards.

7. HIPAA, in general, applies to healthcare providers and those health care providers that conduct certain health care transactions electronically, and HIPAA Business Associates, and sets standards for Defendant's maintenance of Plaintiff's and Class Members' PII and PHI, including appropriate safeguards to be maintained by organizations such as Defendant's to protect the privacy of patient health information, while setting limits and conditions on the uses and disclosures that may be made of such information without express customer/patient authorization.

8. Additionally, the so-called "HIPAA Security Rule" establishes national standards to protect individuals' electronic health information that is created, received, used, or maintained by a HIPAA Business Associate. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. HIPAA provides the standard of procedure by which a medical provider must operate when collecting, storing, and maintaining the confidentiality of PHI and PII.

9. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant knowingly assumed legal and equitable duties to those individuals, including those arising from common law principles.

10. Nonetheless, Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take, implement, and ensure adequate and reasonable measures regarding the safeguarding of Plaintiff's and Class Members' PII and PHI, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data. As a result, and upon information and belief, the PII and PHI of Plaintiff and Class Members has been compromised and they have been and shall be damaged through access by and disclosure to an unknown and unauthorized entity—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future. In

addition, Plaintiff and Class Members, who have a continuing interest in ensuring that their information is safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff

11. Plaintiff Charmeny Lyons is, and at all relevant times was, a resident of Racine, Wisconsin, who has received medical care as a patient of Ascension Health through providers in Racine, Wisconsin. As a result of Defendant's website notice of the Data Breach as alleged below, Plaintiff is concerned about suspicious activity and credit reporting, has been forced to spend time monitoring personal financial accounts for signs of fraudulent transactions or activity, and anticipates that she will continue to have to do so.

Defendant

12. Defendant Ascension Health is a corporation organized under the laws of the state of Missouri. Ascension, a health care system and health care related entity, maintains its principal place of business at 4600 Edmundson Road, St. Louis, Missouri.

JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction over this case under 28 U.S.C. § 1332(d), because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interests and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

2. This Court has general personal jurisdiction over Defendant because Defendant maintains healthcare facilities in this district and conducts substantial business in or from this district.

3. This Court is the proper venue for this action because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District, and because Defendant conducts a substantial part of their business within this District.

FACTUAL BACKGROUND

The Data Breach

4. Plaintiff, and the putative members of the Class, have received medical/health care services as a patient of a provider within the Ascension Health system of medical providers and hospitals.

5. In the course of receiving health care services from Defendant, Plaintiff provided it with her sensitive and HIPAA protected Private Information, which she was required to provide in order to receive such services.

6. No doubt aware of its obligations as an entity doing business within the health care space, in the course of collecting Plaintiff's and class members Private Information, Defendant promised via its privacy policy and required statutory privacy requirements to provide confidentiality and adequate security with respect to such information. To that end, Defendant's website assures patients that "[t]he Site has security measures in place to protect against loss, misuse, or alteration of information under our control.[4]

7. On May 9, 2024, in a notice posted on its website (the "Online Notice"), Defendant informed Plaintiff and Class Members that:

> On Wednesday, May 8, we detected unusual activity on select technology network systems, which we now believe is due to a cybersecurity event. At this time we continue to investigate the situation. We responded immediately, initiated our investigation and activated our remediation efforts. Access to some systems have been interrupted as this process continues.
>
> Our care teams are trained for these kinds of disruptions and have initiated procedures to ensure patient care delivery continues to be safe and as minimally impacted as possible. There has been a disruption to clinical operations, and we continue to assess the impact and duration of the disruption.
>
> We have engaged Mandiant, a third party expert, to assist in the investigation and remediation process, and we have notified the appropriate authorities. Together, we are working to fully investigate what information, if any, may have been affected by the situation. Should we determine that any sensitive information was affected, we will notify and support those individuals in accordance with all relevant regulatory and legal guidelines.[5]

---

[4] https://about.ascension.org/privacy, last visited May 23, 2024.

[5] https://about.ascension.org/en/cybersecurity-event, last visited May 23, 2024.

8. The "disclosure," of the Data Breach amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Omitted from the Online Notice were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

9. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members and failed to adhere to the standard of care required of healthcare related business and services, ultimately leading to and causing the exposure of Private Information.

10. Upon information and belief, the exfiltrated data was not encrypted or similarly secured, allowing nefarious actors easy access to the data.

11. Upon information and belief, Defendant continues to inadequately secure or maintain Plaintiff's PHI and PII, as well as that of all other Class Members.

12. Beyond acknowledging the Data Breach – albeit inadequately – Defendant has not taken or provided therapeutic steps, has failed to adequately compensate Plaintiff and members of the Class, and has failed to adequately address the multiple years of identity theft and financial fraud that Data Breach victims face. As a consequence of the Data Breach, Plaintiff and Class Members will be forced to pay out-of-pocket for necessary identifying monitoring services for years thereafter.

Ascension is Obliged to Preserve and Protect PHI and PII

13. Defendant acquired, collected, stored, and assured the security of, the Private Information of Plaintiff and the Class.

14. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. The information collected, acquired, and stored by Defendant included the Private Information of Plaintiff and Class Members.

15. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII/PHI.

16. At all times material, Defendant was under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. To that end, Defendant was reposed with a legal duty created by HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

17. By obtaining, collecting, using, and storing Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure. And given the highly sensitive nature of the PII and PHI it possessed and the sensitivity of the medical and health services it provides, Defendant had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' PII and PHI.

18. Defendant retains and stores this Private Information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its services.

19. Defendant's failure to adequately safeguard the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

20. Defendant was not permitted to disclose Plaintiff's and Class Members' Private Information for any reason that would apply in this situation.

21. Defendant was obliged by contract, industry standards, common law, and promises and representations made to Plaintiff and Class Members, to keep their Private Information confidential and protect it from unauthorized access and disclosure.

22. Plaintiff and Class Members had a reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep the Private Information they provided confidential and secure from unauthorized access and disclosure.

23. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, consequently enabling and causing the exposure of Private Information of thousands of individuals.

24. Because of Defendant's negligence and misconduct in failing to keep the accessed information confidential, the unencrypted Private Information of Plaintiff and Class Members has been expropriated by unauthorized individuals who can now exploit the PHI and PII of Plaintiff and Class Members and use it as they please.

25. Plaintiff and Class Members now face a real, present and substantially increased risk of fraud and identity theft and have lost the benefit of the bargain they made with Defendant when receiving services.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

26. The PII and PHI of consumers, such as Plaintiff and Class Members, is highly valuable and has been commoditized in recent years.

27. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended

period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

28. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

29. Plaintiff and Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the information in possession of Defendant;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

30. Moreover, Plaintiff and Class Members have an interest in ensuring that Defendant implements reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendant is encrypted, fully secure, remains secure, and is not subject to future theft.

31. As a further direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

32. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized access of and disclosure or risk of exfiltration of Plaintiff's and Class Members' Private Information, Plaintiff and Class Members have suffered, and will continue to suffer, actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they have spent or must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed by unauthorized cyber-thieves in the Data Breach.

Defendant was Well Aware of the Threat of Cyber Theft and Exfiltration in the Healthcare Industry

33. Defendant was aware of the significant repercussions that would result from their failure to protect Private Information and knew, or should have known, the importance of

safeguarding the Private Information entrusted to them and of the foreseeable consequences of a breach of data security.

34. Defendant could have prevented the Data Breach by assuring that the Private Information at issue was properly secured. Defendant's overt negligence in safeguarding Plaintiff's and Class Members' PII and PHI is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as entities in the healthcare space, Defendant was on notice that companies in the healthcare industry are targets for data breaches.

35. The healthcare industry in particular has experienced a large number of high-profile cyberattacks. Cyberattacks, generally, have become increasingly more common. In 2021, a record 715 healthcare data breaches reported, an increase of approximately 100% since 2017.[6]

36. This trend continued in 2022, with 707 healthcare breaches reported, still near record highs.[7] Additionally, according to the HIPAA Journal, the five largest healthcare data breaches reported in 2022 impacted the healthcare records of approximately 13.3 million people.[8] Thus, Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[9]

---

[6] 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed May 23, 2024).

[7] *Id*.

[8] *Id*.

[9] Rebecca Pifer, Tenet says 'cybersecurity incident' disrupted hospital operations, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-sayscybersecurity-incident-disrupted-hospital-operations/622692/ (last accessed May 23, 2024).

Indeed, HHS's cybersecurity arm has issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[10]

37. In the context of data breaches, healthcare is "by far the most affected industry sector."[11] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[12]

38. A TENABLE study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."[13]

39. This is such a breach of cybersecurity where highly detailed PII and PHI records maintained and collected by a healthcare entity were accessed and/or acquired by a cybercriminal.

40. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operations with the resources to put adequate data security protocols in place and assure the security of the data collected by them and entrusted to them by Plaintiff and Class Members.

41. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII and PHI from being compromised.

---

[10] *Id*. (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June - nearly three a day.").

[11] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed May 23, 2024).

[12] *Id.*

[13] *Id.*

Data Breaches Can be Prevented by Entities Such as Ascension

42. Ascension could have prevented this Data Breach for example, among other things, it could have adequately encrypted or otherwise protected their equipment and computer files containing Private Information.

43. The Federal Bureau of Investigation has stated that "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[14]

44. There are a number of measures the United States Government has recommended by implemented to prevent and detect cyber-attacks and/or ransomware attacks, including the following:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

[14] How to Protect Your Networks from RANSOMWARE, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[15]

45. The Microsoft Threat Protection Intelligence Team recommends to following measures that Ascension could have implemented to safeguard against, prevent, and detect cyber-attacks:

Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

[15] *Id.* At 3-4.

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[16]

46. Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

47. Defendant failed to adequately implement one or more of these recommended measures to prevent cyberattacks. The Data Breach by which data thieves acquired and accessed the Private Information of, upon information and belief, thousands of individuals, including that of Plaintiff and Class Members, was a direct and proximate result of Defendant's failure.

Defendant's Conduct Fails to Adhere to Industry Standards, HIPAA and HITECH Standards, and Commensurate Duties it Owed to Plaintiff and the Class

48. Defendant embraced a standard of care and commensurate duty defined by HIPAA, state law and common law to safeguard the PHI and PII of Plaintiff and Class Members.

49. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data under the condition and implied promise and assurance by Defendant that it would keep such Private Information confidential and secure. Accordingly, Defendant also had an implied duty to safeguard their data, independent of any statute.

[16] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a preventable-disaster/, last visited May 23, 2024.

50. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

51. On information and belief, Defendant is a business associate pursuant to HIPAA.

52. Defendant is also regulated by the Health Information Technology Act ("HITECH").[17] See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

53. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

54. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

55. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

56. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

57. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

---

[17] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

58. HIPAA's Security Rule requires Defendant to do the following:

a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c) Protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and

d) Ensure compliance by its workforce.

59. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

60. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

61. Plaintiff's and Class Members' Personal and Medical Information, including their PII and PHI, is "protected health information" as defined by 45 CFR § 160.103.

62. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

63. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

64. Plaintiff's and Class Members' personal and medical information, including their PII and PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

65. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

66. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

67. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

68. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

69. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

70. HIPAA requires covered entities and business associates to protect against reasonably anticipated threats to the security of sensitive patient health information.

71. Covered entities and business associates must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

72. This Data Breach constitutes an unauthorized access of PHI, which is not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

73. The Data Breach could have been prevented if Defendant had implemented HIPAA mandated and industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients with respect to adequately securing and maintaining the confidentiality of Private Information.

74. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiff's and Class Members' PII and PHI.

75. Upon information and belief, prior to the Data Breach, Defendant was aware of its security failures but failed to correct them or adequately and timely disclose them to the public, including Plaintiff and Class Members.

76. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

77. Because Defendant failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII and PHI of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' PII and PHI remains at risk of subsequent Data Breaches.

78. In addition to their obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiff and Class Members.

79. Defendant owed a duty to Plaintiff and Class Members to ensure that the Private Information it collected and was responsible for was adequately secured and protected.

80. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

81. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

82. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

83. Defendant owed a duty to Plaintiff and Class Members to disclose if its data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendant.

84. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

85. Defendant owed a duty to Plaintiff and Class Members to mitigate the harm suffered by the Representative Plaintiff's and Class Members' as a result of the Data Breach.

86. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system and safeguards to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits;

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

g. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information;

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons; and

k. Retaining information past a recognized purpose and not deleting it.

The Federal Trade Commission Defines Defendant's Conduct as Constituting Unfair or Deceptive Acts

87. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

88. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[18]

89. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, encrypt information stored on networks, understand its network's vulnerabilities, and implement policies to correct any security problems.[19]

[18] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf, last visited May 23, 2024.

[19] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business last visited May 23, 2024.

90. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

91. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice.

92. Defendant was at all times fully aware of its obligations to protect Plaintiff's and Class Members' Private Information because of their business models of collecting and storing Private Information. Defendant was also aware of the significant adverse repercussions befalling healthcare recipients that would result from its failure to do so.

Value of the Relevant Sensitive Information

93. Although they provide greater efficiency and cost savings for providers, electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cyber criminals seeking to access them. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PII and PHI and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

94. The high value of PII and PHI and financial information to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price

ranging from $40 to $200, and bank details have a price range of $50 to $200.[20] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[21]

95. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[22] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[23] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[24]

96. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

97. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

---

[20] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-darkweb-how-much-it-costs/ last accessed May 23, 2024.

[21] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ last visited May 23, 2024.

[22] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 last visited May 23, 2024.

[23] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ last visited May 23, 2024.

[24] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches last visited May 23, 2024.

98. Identity thieves can use PII and PHI and financial information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

99. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

100. The harm to Plaintiff and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical- related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[26]

101. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy

---

[25] 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf last visited May 23, 2024.

[26] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ last visited May 23, 2024.

Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[27]

102. If cyber criminals manage to access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiff and Class Members.

103. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[28] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[29]

104. Data breaches are preventable.[30] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[31] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[32]

105. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information

---

[27] *Id.*

[28] *See* Elinor Mills, Study: Medical Identity Theft is Costly for Victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ last visited May 23, 2024.

[29] *Id.; see also* Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, available at https://www.experian.com/blogs/ask-experian/healthcare-data-breachwhat-to-know-about-them-and-what-to-do-after-one/ last visited May 23, 2024.

[30] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[31] *Id.* at 17.

[32] *Id*. at 28.

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[33]

106. The Data Breach resulted from a combination of insufficiencies that demonstrate how Defendant failed to comply with industry, standards, safeguards and concomitant duties established by HIPAA regulations.

Loss of the Benefit of the Bargain

107. As a consequence of Defendant's inadequate data security systems and protection, Plaintiff and Class Members have been deprived of the benefit of their bargain which occurred when they agreed to receive services administered by Defendant. Plaintiff and Class Members, reasonable consumers – understandably expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant had not provided the necessary adequate data security in any event. Consequently, Plaintiff and Class Members received services that were of a lesser value than what they had reasonably expected from and bargained for with Defendant.

Ongoing Need for Expensive Credit and Identity Theft Monitoring

108. Unquestionably there will be a future cost of credit and identify theft monitoring that will be necessary for Plaintiff and Class Members' protection going forward as a consequence of the Data Breach and the sensitive Private Information that has been accessed. The probability is strong that the stolen information will be used by criminals to accomplish crimes based on identity theft, including opening bank accounts and victims' names to make purchases or launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims. These fraudulent incidents may not be detected for years and individuals may not even know that they have yet occurred.

---

[33] *Id.*

109. Credit monitoring and identity theft monitoring is expensive. The cost can run approximately $200 a year per each Class Member. This cost is necessary and reasonable, for Plaintiff and Class Members are now forced to monitor and protect themselves from identity theft going forward, and need to do so for many years.

110. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.8% of U.S.-based workers are compensated on an hourly basis, while the other 44.2% are salaried.[34]

111. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[35] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[36] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

112. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

CLASS ALLEGATIONS

---

[34] U.S. BUREAU OF LABOR STATISTICS, Characteristics of minimum wage workers, 2021, available at https://www.bls.gov/opub/reports/minimum-wage/2021/pdf/home.pdf, last visited May 23, 2024; *see also*, Bureau of Labor Statistics, https://www.bls.gov/news.release/empsit.t19.htm, last visited May 23, 2024 (finding that on average, private-sector workers make $1,146.99 per 40-hour work week).

[35] *See* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html last visited May 23, 2024.

[36] *Id.*

113. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff assert common law and statutory claims, as more fully alleged hereinafter, on behalf of the following Nationwide Class, and Wisconsin Class, defined as follows:

> **Nationwide Class:** All residents of the United States whose PII or PHI was accessed or otherwise compromised as a result of the Ascension Health Data Breach.
>
> **Wisconsin Class:** All residents of the state of Wisconsin whose PII or PHI was accessed or otherwise compromised as a result of the Ascension Health Data Breach.

114. Members of the Nationwide Class, and Wisconsin Class are referred to herein collectively as "Class Members" or "Class."

115. Excluded from the Class are Defendant, any entity in which Defendant have a controlling interest, and Defendant' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

116. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

117. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but the Defendant's health system includes thousands of providers and numerous medical centers. Ascension acknowledges that in fiscal year 2023 that its providers had 16.4 million physician office and clinic visits and that 599,000 surgeries were held at its facilities, indicating that the potential number of individuals affected by the Data Breach, the members of the Class, includes thousands of people, making joinder of each individual impracticable. Ultimately, members of the Class will be readily identified through Defendant' records.

118. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class Members' PII and PHI;

b) Whether Defendant failed to protect Plaintiff's and the Class Members' PII and PHI, as promised;

c) Whether Defendant's computer system systems and data security practices used to protect Plaintiff's and the Class Members' PII and PHI violated HIPAA, federal, state and local laws, or Defendant' duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff and the Class Members' PII and PHI properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, state privacy statutes, and state medical privacy statutes, HIPAA, and/or FTC law or regulations, imposing duties upon Defendant, applicable to Plaintiff and each of the Class;

f) Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class Members' PII and PHI;

h) Whether Defendant entered into contracts with Plaintiff and the Class Members that included contract terms requiring Defendant to protect the confidentiality of Plaintiff's PII and PHI and have reasonable security measures;

i) Whether Defendant conduct described herein constitutes a breach of their express or implied contracts or covenants, or agreements with Plaintiff and the members of each Class;

j) Whether Defendant should retain the money paid by Plaintiff and members of each of the Class to protect their PII and PHI;

k) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant' wrongful conduct;

l) Whether Plaintiff and the Class Members are entitled to restitution as a result of Defendant' wrongful conduct;

m) What equitable relief is appropriate to redress Defendant' wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

119. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the Class Members sustained damages as a result of Defendant' uniform wrongful conduct during transactions with them.

120. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interest antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

121. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Ascension database still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the Defendant's database.

122. **Class-wide Applicability**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

123. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class against Defendant)

124. Plaintiff, on behalf of the Class, re-alleges and incorporates the above allegations by reference.

125. Plaintiff and Class Members were required to submit Private Information to healthcare providers, including Defendant, in order to obtain insurance coverage and/or to receive healthcare services.

126. Defendant knew, or should have known, of the risks and responsibilities inherent in collecting and storing the Private Information of Plaintiff and Class Members.

127. As described above, Defendant owed duties of care to Plaintiff and Class Members whose Private Information had been entrusted to Defendant.

128. Defendant breached its duties to Plaintiff and Class Members by failing to secure their Private Information from unauthorized disclosure to third parties.

129. Defendant acted with wanton disregard for the security of Plaintiff and Class Members' Private Information.

130. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members because they collected and/or stored the Private Information of Plaintiff and the Class Members.

131. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

132. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known it was failing to meet its duties, and that Defendant's breach of such duties would cause patients such as Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their Private Information.

133. As a direct and proximate result of Defendant' negligent and reckless conduct, Plaintiff upon information and belief, and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class against Defendant)

134. Plaintiff, on behalf of the Class, re-alleges and incorporates the above allegations by reference.

135. Pursuant to HIPAA (42 U.S.C. §1302d *et. seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Personal Information.

136. Defendant breached their duties to Plaintiff and Class Members under HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information, *i.e.,* by affirmatively sharing Plaintiff's Private Information, without Plaintiff's authorization, with third parties.

137. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

138. But for Defendant's wrongful and negligent breach of its aforesaid duties, Plaintiff and Class Members would not have been injured.

139. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach of those duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized disclosure of their Private Information.

140. As a direct and proximate result of Defendant's negligent conduct and reckless, Plaintiff upon information and belief, and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class against Defendant)

141. Plaintiff, on behalf of the Class, re-alleges and incorporates the above allegations by reference.

142. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with Defendant, as alleged above.

143. The contracts respecting which Plaintiff and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiff's Private Information from unauthorized disclosure and to comply with state laws and regulations.

144. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members who sought medical services or treatment at Ascension affiliated facilities and, in doing so, entrusted Defendant, pursuant to its requirements and Notice of Privacy Practices, with their Private Information.

145. Despite this special relationship with Plaintiff, Defendant did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' Private Information.

146. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

147. Accordingly, Plaintiff, upon information and belief, and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class against Defendant)

148. Plaintiff, on behalf of the Class, re-alleges and incorporates the above allegations as if fully set forth herein.

149. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Personal Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and do store.

150. Defendant had and continues to have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep secure their Private Information from disclosure without authorization from Plaintiff and the Class Members.

151. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

152. Plaintiff, upon information and belief, and Class Members have been injured as a direct and proximate result of Defendant's breach of its fiduciary duties and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT V
Breach of Implied Contract
(On behalf of Plaintiff and the Class against Defendant)

13. Plaintiff, on behalf of the Class, re-alleges and incorporates the above allegations by reference.

14. Defendant required Plaintiff and the Class to provide and entrust their PII/PHI as a condition of obtaining medical care and medical devices from Defendant.

15. Plaintiff and the Class paid money to Defendant in exchange for goods and services, as well as Defendant's promise or obligation to protect their protected health information and other PII from unauthorized disclosure.

16. Defendant promised and/or was bound by law to comply with HIPAA and HITECH standards and to make sure that Plaintiff's and Class Members' protected health information and other PII would remain protected.

17. Through its course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII/PHI and financial information.

18. Defendant required Plaintiff and Class Members to provide and entrust their PII/PHI, including for example, medical information, record or account numbers, names, Social Security numbers, email addresses, and dates of birth.

19. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide its PII/PHI to Defendant, in exchange for, amongst other things, the protection of their PII/PHI. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

20. Plaintiff and the Class Members would not have entrusted their PII/PHI to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

21. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

22. Defendant breached the implied contracts it made with Plaintiff and the Class by making their PII/PHI accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the PII/PHI was secure, failing to encrypt Plaintiff and Class Members' sensitive PII/PHI, failing to safeguard and protect their medical, personal and financial information and by failing to provide timely and accurate notice to them that medical and personal information was compromised as a result of the data breach.

23. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise or obligation under the law to abide by HIPAA and HITECH.

24. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

25. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

26. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

27. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

28. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

29. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

30. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530©.

31. Defendant further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII/PHI.

32. Defendant's failures to meet its promises and/or obligations constitute breaches of the implied contracts.

33. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) and/or actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) and/or the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

34. As a result of Defendant's breach of implied contract, Plaintiff and the Class Members are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class pursuant to Section 382 of the Code of Civil Procedure, appointing Plaintiff as representative of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: May 24, 2024

Respectfully submitted,

BARRACK, RODOS & BACINE

/s/ Stephen R. Basser
Stephen R. Basser
Samuel M. Ward
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

sbasser@barrack.com
sward@barrack.com

Counsel for Plaintiff Charmeny Lyons